Privacy and Technology Workshop
Edinburgh, September 2005

The Problem With Privacy – A Modest Proposal

Lilian Edwards
Co-Director, AHRC Centre in Intellectual Property and Technology Law
University of Edinburgh

L.edwards@ed.ac.uk
www.law.ed.ac.uk/ahrb

Background: Privacy, trust and e-commerce

- Consumer trust in buying on-line, and protection of on-line privacy are usually regarded as intimately connected
- Eg 84% of EU consumers refused to shop on-line in 2004, 25% citing lack of trust of medium (Eurobarometer)
- Underlying aim of regulation of privacy *for on-line environment specifically* is to expressly promote confidence and trust in the new medium by consumers.
- Thesis of paper is that current EU legal regulation fails to do so, as it fails to prevent privacy related harms in on-line transactions; a post-harm regime of compensation is alternative proposal

What are the privacy harms to consumers from disclosing data on line?

- *Identity theft harms* eg misuse of credit card info. Up 45% in UK last year (APACS, March 04). Over ½ million complaints re ID theft to FTC in 2003.
- *Disclosure harms* eg Eli Lilly Prozac list, wrongful credit info, sale of preference lists
- *Invasion harms*: eg spam (now up to 62% all email, Brightmail, Feb 04), pop-up ads, spyware, etc.

However

- Consumers gain convenience factor, personalisation and trust from data collection eg Amazon, locational data
- Data collecting and processing businesses gain assets of value

EC Data Protection regime : problems

- **Historical origins:** DP tailored for mainframe, non-Internet, data warehousing environment, when compliance by few "elephants" (Swire), as opposed to many "mice", was relatively easy to police.
- **The sheer size of cyberspace and lack of resources for compliance:** Post Internet, many 1,000,000 s of "mice". Data Protection Commissioners generally under-funded, under-staffed, reactive, not pro-active.
- **The global cyberspace environment**: Most processing of personal info goes on outside EU (around 90% of spam from outside EU) yet no global harmonisation on DP law. Rapprochement exercises such as EU/US Art 25 DPD "safe harbor" not outstanding successes (only 493 US companies signed up at April 04.)
- **Lack of customer pressure to enforce** : consumer level of knowledge and exercise of DP rights, and of risks of giving away personally info generally, very low.
- **Does not fit US or EU corporate business models of data sharing** after mergers, take-overs, liquidations etc. Also costly & fiddly. US business unwilling to regard data as property of consumer; EU businesses regard it as compliance hurdle and annoying business cost engaged by trading worldwide.

US Alternative – law/norms

- US – mainly commercial self regulation, some piecemeal legislation on sensitive data. Privacy policies semi-mandatory. On line self-regulatory bodies – trust marks or kite marks – TrustE, Online Privacy Alliance etc,
- Some (increasing) FTC compliance action
- Poor past record of compliance by trust seal members and query over effective sanctions
- No real marketplace of choice in privacy policies
- Generally seen as inadequate by EU model
- Industry hostility to costs of full DP regime
- Personal data seen as *property of collector, not subject*

Market/Code Solutions

Deighton “a market mechanism to allocate privacy to those who value it is, at present.. a very imperfect method”

Eg loyalty points, Air Miles,

Eg P3P : in theory, code which enables consumer to bargain as to when and why they will allow their personal information to be collected, via pre-selections on security made in browser

But P3P is essentially just automated bargaining, which requires a real marketplace of choices in privacy to work (the “lemon” problem) , plus savvy consumers, plus a regulatory background for enforcement of terms of contract

Issues:

- No post-collection enforcement
- consumers can’t bargain fairly when they don’t know the value of their personal information, especially in aggregate
- consumers won’t care enough to learn how to use P3P
- little or no actual choice on the privacy market

“Real” PETS do offer genuine privacy safeguards – but are rarely used for commercial not political privacy.

A modest proposal

The "privacy contribution": abandoning control in favour of compensation

- Inspired partly by Terry Fisher's approach to P2P illegal file sharing/downloading problem
- Fisher advocates *giving up* futilely trying to control illegal copying of copyright work by rights-holders – instead, give work away, abandon trying to enforce copyright rules against downloaders. Benefits of "semiotic democracy".
- BUT – still provide *compensation* to rights-holders via an appropriate *levy* eg on broadband, computer hardware, blank CDs – re-distributed fairly in proportion to downloads
- Transfer to privacy context – instead of trying (unsuccessfully) to *prevent* privacy harms by rigorous DP rules, consumers get *compensated* for privacy harms. But retain benefits of data flow.

In privacy context – who should pay contribution?

- A. – the businesses who make money out of collecting and processing data and currently get it (largely) for free. Some kind of “privacy contribution”. (Issues: how much value added to data? What about false data supplied?)
- *Clearly not ideal* to only compensate breaches, not prevent them. Does not reflect EU view of privacy as inherent to human dignity rather than property right. NB Human rights of those who care deeply about privacy still need attention.
- BUT - If data collectors and processors are made to pay incremental premium for responsibility for privacy harms, they will be incentivised to try harder to *improve* privacy
- And more effective than ordinary negligence model, because enforcement will be by well resourced independent body (as in DP), not left up to individual consumer (and no need to track down mice)

Compensating privacy harms

- How is the "privacy contribution" to be used?
  - Provide statutory fixed-rate compensation pay-outs for recognised privacy harms, reported to and accredited by enforcement body. *No need to prove fault,* causality, no intervening 3rd party. No need for consumers to bring own actions. Data collectors who pay contribution can retain common law rights to pursue actual wrong-doers to compensate themselves.
  - Improve enforcement. Create new watchdog body, or top up funding of existing national bodies such as FTC, national DPCs, to aid in compliance with national laws/self regulation measures
  - Provide PETS for free (and public education) to consumers who *refuse* to give away personal info as is their human right ("inalienability" controls on commodification, per Schwartz, 2004)

Benefits

- Goes after “elephants” (visible data collecting businesses) not “mice” (spammers, ID thieves etc) to get remedies for those harmed
- Focus is on *external effects of data collecting/processing* – not “indoor management” of companies. Aim is to provide *remedies for harms* not to require/enforce internal bureaucratic regime.
- Retains advantages of data disclosure/sharing/free flow for consumers and businesses, while minimising, or at least compensating for, privacy harms
- May in end thus create greater trust in e-commerce?

Criticisms

- Why *should* the "elephants" agree to pay for the sins of the "mice"?
  - Natural justice - currently personal information is largely a "free gift" to them
  - Pragmatic argument –contributors are those most closely connected to the data processing which leads to privacy harms, therefore paying contribution will encourage them to improve in-house privacy standards
  - PR incentive – putting what is effectively an industry "no fault" compensation scheme in place will reassure consumers enormously and engender trust? hence increase e-commerce uptake? Cf "Tylenol" trust-wrap solution (Swire) & Doctorow "sell privacy as a feature"
  - Reduction of red tape incentive – *quid pro quo* of no longer having to comply with DP notification, access requests and other compliance fuss. No more interference with "indoor management", esp good for multinationals.
  - Could be transitional device till technology/code catches up with better solutions – eg one-off credit card numbers, buying "anonymous browser IDs", distributed pseudonymity